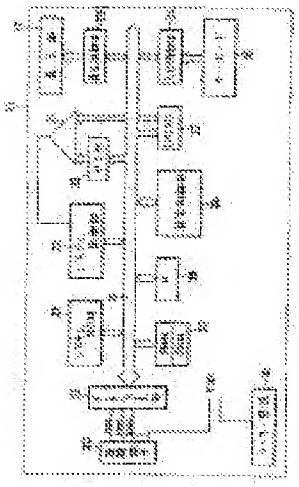
Publication number:	JP62015657 (A)
Publication date:	1987-01-24
Inventor(s):	SUZUKI HIDEO
Applicant(s):	CASIO COMPUTER CO LTD
Classification:	
- international:	G07F7/12; B42D15/10; G06K17/00; G06K19/077; G06Q20/00; G06Q40/00; G07D9/00; G07F7/10; H04M1/675; G07F7/12; B42D15/10; G06K17/00; G06K19/077; G06Q20/00; G06Q40/00; G07D9/00; G07F7/10; H04M1/66; (IPC1-7): G06F15/30; G06K17/00; G07F7/08
- European:	G06K19/077; G07F7/10D6P; G07F7/10D8; H04M1/675
Application number:	JP19850153637 19850712
Priority number(s):	JP19850153637 19850712

Also published as:

- JP8003821 (B)
- JP2090978 (C)
- US4742351 (A)

Abstract of **JP 62015657 (A)**

PURPOSE:To approve the propriety of the owner of an IC card by providing a means inputting the character number information into the IC card in a no- connection state with an external device and collating the input information with the identification information on an identification memory within the IC card. CONSTITUTION:When the IC card 11 is put into a card slit at an IC card terminal, the account number PAN and a ciphered account number PAN' sent from the card side are decoded at the terminal side. When the coincidence is obtained between the PAN and the PAN', it is decided that the card 11 is right. Then the card 11 is pulled out of the terminal and an identification number PIN is supplied by means of a PIN key through the keyboard 16 of the card 11.; Then the input PIN of a PIN latch part 28 is collated with the number PIN of the genuine card owner stored in a PIN memory 27 through an identification information comparing part 31. When the coincidence is obtained from this collation, it is decided that the input operator of the PIN key is identical with the genuine owner of the card 11.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－15657

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和62年(1987)1月24日
G 06 F 15/30		8219－5B	
G 06 K 17/00		6711－5B	
G 07 F 7/08		B－7234－3E	審査請求　未請求　発明の数 1　（全9頁）

⑤4発明の名称　ＩＣカードにおける本人照合方式

⑳特　願　昭60－153637

㉒出　願　昭60(1985)7月12日

⑦2発明者　鈴木　秀夫　東京都西多摩郡羽村町栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内

⑦1出願人　カシオ計算機株式会社　東京都新宿区西新宿２丁目６番１号

明　細　書

１．発明の名称

ＩＣカードにおける本人照合方式

２．特許請求の範囲

外部装置との接続によりカード自体の正当性が調べられるＩＣカードにおける本人照合方式において、上記ＩＣカード内に設けられ所定文字数の暗証情報を予め記憶する暗証情報メモリと、上記外部装置との非接続状態においてのみ上記ＩＣカードにて上記所定文字数の情報を入力可能とする手段と、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをＩＣカード内にて比較照合する手段と、この比較照合手段による暗証情報の照合結果を出力する手段とを具備し、上記ＩＣカードの正当性を確認すると共に、上記暗証情報が上記外部装置に一切入力されることなく、カード所有者の本人照合を行なうことを特徴とするＩＣカードにおける本人照合方式。

３．発明の詳細な説明

［発明の技術分野］

この発明は、ＩＣカードの正当性およびそのカード所有者が本人か否かを確実に認証するＩＣカードにおける本人照合方式に関する。

［従来技術とその問題点］

近年はキャッシュレス時代と呼ばれており、クレジットカード会社等により発行されたカードを使用することにより、現金の取扱いをせずに商品の購入が可能となっている。上記カードとしては、従来、プラスチックカード，エンボスカード，磁気ストライプカード等が一般に使用されているが、これらのカードは構造上偽造が簡単であり、不正使用が問題になっている。このような問題を解決するため、最近ではカード内に、暗証番号等を記憶したＩＣ回路を組込み、暗証番号が外部から容易に読出せないようにした情報カード、所謂ＩＣカードが開発されている。このＩＣカードは偽造が困難で機密性に優れ、また、多数の情報を記憶できるという利点がある。しかして、上記のようなＩＣカードを使用して実際に取引を行なう場合

には、銀行あるいは商店等に設置したＩＣカードターミナルにＩＣカードを装着し、暗証番号等を入力してカードおよびカード所有者の正当性を確認した後、所定の処理動作が行なわれるようにしている。

しかしながら、このようにＩＣカードをターミナルに装着して暗証番号の照合を行なう場合、第１に、例えば商店等において暗証番号を入力する際に、その入力操作自体を視覚によって盗まれる可能性がある。また、第２に、例えばターミナル側に、カード所有者によって入力される暗証番号の情報を、暗証番号一致の信号を待って記憶する細工が施してある場合、真のカード所有者の暗証番号が上記ターミナルの設置される商店主等によって、簡単に盗まれてしまう恐れもある。ここで、上記第１の問題点については、カード所有者自体がキー操作時に自分の暗証情報を盗まれないように気を付ければよいわけであるが、第２の問題点については、カード所有者側における対策は全く立てられないものである。

そこで現在、カード所有者の暗証番号をカード発行時において予めカード内メモリに記憶させ、カード本体に設けたキーボードより入力される暗証番号と、上記メモリ内暗証番号とを比較照合し、その照合結果を即座にＩＣカード自体に設けた表示部にて表示するようにした、所謂、ターミナル側とは全く接続関係を持たないで、独自に本人照合を行なうことのできるＩＣカードが考えられている。しかし、このような単独にて本人照合を行なえる機能を有するＩＣカードにあっても、そのカード自体が偽造される可能性がある。すなわち、カード本体上の表示部にて、例えば「本人ＯＫ」等の表示が行なわれたとしても、そのカード自体、真に正当のカード会社より発行されたものかどうかを確認することができないため、結局、真のカード所有者の認証を行なうのは非常に困難なものとなる。

［発明の目的］

この発明は上記のような問題点に鑑みなされたもので、カード所有者の暗証情報が不正に盗まれてしまうことなく、カード所有者の正当性を確実に認証することができるようになるＩＣカードにおける本人照合方式を提供することを目的とする。

［発明の要点］

すなわちこの発明に係わるＩＣカードにおける本人照合方式は、外部装置との接続によりカード自体の正当性が確認できるＩＣカード内に、所定文字数の暗証情報を予め記憶する暗証情報メモリを設けると共に、上記外部装置との非接続状態において上記所定文字数情報の入力可能な手段を備えさせ、そして、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをこのＩＣカード内にて比較照合し、その照合結果を出力するように構成したものである。

［発明の実施例］

以下図面によりこの発明の一実施例を説明する。

第１図はそのＩＣカードにおける本人照合方式を実現したＩＣカード１１およびその外部装置（ＩＣカードターミナル）１２の外観構成を示すもので、本方式におけるターミナル１２には、その本体上面にキーボード１３、表示部１４および上記ＩＣカード１１との電気的接続を図るためのカード挿入口１５が設けられている。

第２図は、上記ＩＣカード１１の外観構成を示すもので、このＩＣカード１１には、その本体上面にキーボード１６、表示部１７およびソーラ電池１８が設けられている。上記キーボード１６は、テンキー、ファンクションキー等の演算用キーと共に、ＰＩＮキー１９を備えている。上記ＰＩＮキー１９は、本カード１１とカード所有者との照合を行なう際に、その本人の暗証番号ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）を入力するのに使用されるもので、この暗証番号ＰＩＮは、カード所有者により任意に設定される所定文字数のコードである。また、このＩＣカード１１の本体上面には、さらに接続端子２０を設け、銀行等の金融機関あるいは商店の店頭等に設置される上記ターミナル１２側との接続を図れるようにする。

次に、第３図により上記ＩＣカード１１の回路構成について説明する。

同図において２１はバスラインで、このバスライン２１には、システム制御部２２、システムＲＯＭ２３、キーボード１６の制御を行なう入力制御部２４、表示部１７の制御を行なう表示制御部２５および演算制御部２６が接続される。また、このバスライン２１には、ＰＩＮメモリ２７、ＰＩＮラッチ部２８、フラグレジスタ２９およびＰＡＮメモリ３０が接続される。上記ＰＩＮメモリ２７には、本カード１１の発行時において、カード所有者本人が設定した暗証番号（ＰＩＮ）が予め記憶され、また、ＰＩＮラッチ部２８は、上記キーボード１６にてＰＩＮキー１９を使用してキー入力される所定文字数の情報をラッチするもので、このＰＩＮラッチ部２８と上記ＰＩＮメモリ２７とをそれぞれ暗証情報比較部３１に接続し、この比較部３１からの比較照合出力を上記システム制御部２２に供給する。この場合、システム制御部２２は、上記比較部３１による比較照合出力が一致判定出力であるか否かで、上記フラグレジスタ２９に対してフラグ“１”または“０”を立てさせる。一方、上記ＰＡＮメモリ３０には、予めカード発行者により設定される口座番号ＰＡＮ（Ｐｒｉｍａｒｙ Ａｃｃｏｕｎｔ Ｎｕｍｂｅｒ）およびこの口座番号ＰＡＮが特定のアルゴリズムにて暗号化された暗号化口座番号ＰＡＮ′が記憶されるもので、この暗号化口座番号ＰＡＮ′は、後述するＰＵＫ（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｏｄｅ）により解読されるものである。ここで、上記ＰＩＮメモリ２７およびＰＡＮメモリ３０はそれぞれＥＰＲＯＭにて構成され、一方、ＰＩＮラッチ部２８およびフラグレジスタ２９は、それぞれＲＡＭにて構成される。そしてさらに、上記バスライン２１には、インターフェイス部３２を介して接続端子２０を接続する。このようなシステム制御部２２乃至インターフェイス部３２にて構成されるカード回路は、単独ではソーラ電池１８による電源電圧V_{DD}により、また、上記ターミナル１２との接続時においては、ターミナル１２側から上記接続端子２０を介して供給される電源電圧V_{DD}により駆動される。この場合、上記キーボード１６によるＰＩＮキー１９を使用した所定文字数情報のキー入力動作は、上記ターミナル１２との接続時における電源供給時には、絶対に行なわれないように構成する。

次に、第４図により上記ＩＣカードターミナル１２の回路構成について説明する。

同図において４１はバスラインで、このバスライン４１には、システムＲＯＭ４２、システム制御部４３、キーボード１３を制御する入力制御部４４、表示部１４を制御する表示制御部４５および上記第３図におけるフラグレジスタ２９にフラグ“１”が立ったか否かを判断するフラグ判断部４６が接続される。この判断部４６によるフラグ判断信号は、上記システム制御部４３に供給される。また、このバスライン４１には、本ターミナル１２に接続されるＩＣカード１１からのＰＡＮデータをラッチするＰＡＮラッチ部４７および暗号化口座番号ＰＡＮ′を解読するための解読部４８が接続される。この解読部４８には、上述した暗号解読用のキーコードを記憶するＰＵＫメモリ４９を接続し、このメモリ内のキーコードによって解読した口座番号を（ＰＡＮ′）として解読ＰＡＮラッチ部５０にラッチさせる。そして、この解読ＰＡＮラッチ部５０および上記ＰＡＮラッチ部４７を、それぞれ口座番号比較部５１に接続し、この比較部５１からの比較照合信号を上記システム制御部４３に供給する。そしてさらに、上記バスライン４１には、インターフェイス部５２を介して接続端子５３が接続される。この接続端子５３は、上記第１図におけるカード挿入口１５内に設けられ、電源制御部５４からの電源電圧V_{DD}の供給ラインが接続される。そして、上記のようにシステムＲＯＭ４２乃至インターフェイス部５２により構成されたターミナル回路は、上記電源制御部５４からの電源電圧V_{PP}により駆動される。

次に、上記実施例方式にてＩＣカード１１の正当性およびカード所有者が本人か否かを順次照合

確認する場合の動作を、第５図および第６図に示すフローチャートを参照して説明する。

第５図はＩＣカードターミナル１２内のフローチャートを、第６図はＩＣカード１１内のフローチャートを示すもので、まず始めに、ＩＣカード１１は、ソーラ電池１８による単独の動作状態において、ステップＢ１に示すように、ターミナル１２側からの電源電圧Ｖｄｄの供給が有るか否かを常に検出し判断する。このステップＢ２においてＮ（Ｎｏ）、つまりターミナル１２とは接続状態にないと判断されている場合には、ステップＢ２に進み、キーボード１６によるキー入力データは通常の電卓機能により処理される。

ここで、ステップＡ１において、ＩＣカードターミナル１２のカード挿入口１５に対してＩＣカード１１の一端を挿入し、カード側の接続端子２０とターミナル側の接続端子５３との電気的接続を図ると、ステップＡ２に進み、ターミナル側の電源制御部５４からカード側に対する電圧Ｖｄｄの電源供給が開始される。すると、上記カード側のステップＢ１においてはＹ（Ｙｅｓ）、つまり電源電圧Ｖｄｄが供給されターミナル１２との完全接続状態に至ったと判断されると、ステップＢ３に進み、ＰＡＮメモリ３０より取出した口座番号ＰＡＮおよび暗号化口座番号ＰＡＮ′を、インターフェイス部３２を介してターミナル側に送信する。すると、ターミナル側では、ステップＡ３において、上記カード側より送られて来るＰＡＮおよびＰＡＮ′を受信し、ＰＡＮをＰＡＮラッチ部４７に、ＰＡＮ′を解読部４８に送込む。この解読部４８では、ステップＡ４において、ＰＵＫメモリ４９に記憶される暗号解読用のキーコードに基づき上記暗号化口座番号ＰＡＮ′を解読し、解読ＰＡＮラッチ部５０に（ＰＡＮ′）としてラッチさせるもので、この後ステップＡ５に進み、口座番号比較部５１は、上記ＰＡＮラッチ部４７にラッチされる口座番号ＰＡＮと解読ＰＡＮラッチ部５０にラッチされる解読口座番号（ＰＡＮ′）とを比較照合する。このステップＡ５においてＹ（Ｙｅｓ）、つまりカード側より送られて来るＰＡＮと本ターミナルにて解読した（ＰＡＮ′）とが一致し、現在接続中のＩＣカードは正当なものであると判定されると、ステップＡ６に進み、システム制御部４３は表示部１４に対してカードＯＫメッセージ（ＯＫ！）を表示させる。これにより、まず、上記ＩＣカード１１は、例えば銀行等により正規に発行された正当なＩＣカードであることが確認される。

この後、ステップＡ７に進んで、ＩＣカードターミナル１２よりＩＣカード１１を抜き、各接続端子２０－５４間を非接続状態とすると、ターミナル１２の電源制御部５４によるＩＣカード１１に対する電源電圧Ｖｄｄの供給は停止され、ステップＢ４においてＹ（Ｙｅｓ）と判断される。そして、次に、ステップＢ６に進み、ＩＣカード１１のキーボード１６よりＰＩＮキー１９を使用して暗証番号ＰＩＮをキー入力する。すると、このキー入力によるＰＩＮはＰＩＮラッチ部２８に送込まれてラッチされ、そして、このＰＩＮラッチ部２８にてラッチしたキー入力によるＰＩＮとＰＩＮメモリ２７により予め記憶される本カード１１の真の所有者の暗証番号（ＰＩＮ）とが、ステップＢ７において、暗証情報比較部３１にて照合比較される。ここで、Ｙ（Ｙｅｓ）、つまり、上記ＰＩＮと（ＰＩＮ）とが一致し、上記ステップＢ６におけるＰＩＮのキー入力者は、本カード１１の真の所有者であると判定されると、ステップＢ８に進み、システム制御部２２は表示部１７に対して本人ＯＫメッセージ（ＯＫ！）を表示させる。これにより、現在本カード１１を手中にしている本人が、真のカード所有者であることが確認されるようになり、上記ステップＡ６におけるカード正当性の確認とあいまって、カード所有者の正当性は確実なものとなる。

一方、上記ステップＡ５においてＮ（Ｎｏ）、つまり接続中のカードより送られたＰＡＮと本ターミナルにて解読した（ＰＡＮ′）とが一致せず、現在接続されているカード１１は正規に発行されたものではないと判定されると、ステップＡ８に進み、システム制御部４３は表示部１４に対して

カード不可メッセージ（ＢＡＤ）を表示させる。これにより、上記ＩＣカード１１は、例えば偽造された疑い物の可能性が高いことが確認される。よって、本カード１１の所有者も、このステップＡ８の時点において、正当な所有者ではないことが判明する。

さらに、上記ステップＡ６においてＯＫメッセージが表示されたとしても、上記ステップＢ７においてＮ（Ｎｏ）、つまりＩＣカード１１においてキー入力したＰＩＮと予め記憶される真のＰＩＮとが一致しないと判定されると、ステップＢ９に進み、システム制御部２２は表示部１７に対して本人不可メッセージ（ＢＡＤ）を表示させる。これにより、本ＩＣカード１１が上記ターミナル１２に正規に対応するものであっても、その所有者自体が真の所有者ではないことが確認されるようになる。この場合、本カード１１は、例えば盗難に合った可能性が高いことが判明する。

次に、上記実施例方式にてＩＣカード１１の正当性およびカード所有者が本人か否かを、上記動作とは逆に順次照合確認する場合の動作を、第７図および第８図に示すフローチャートを参照して説明する。

まず、ステップＤ１において、ＩＣカード１１のキーボード１６よりＰＩＮキー１９を使用して暗証番号ＰＩＮをキー入力する。すると、このキー入力によるＰＩＮはＰＩＮラッチ部２８に送込まれてラッチされ、そして、このＰＩＮラッチ部２８にてラッチしたキー入力によるＰＩＮとＰＩＮメモリ２７により予め記憶される本カード１１の真の所有者の暗証番号（ＰＩＮ）とが、ステップＤ２において、暗証情報比較部３１にて照合比較される。ここで、Ｙ（Ｙｅｓ）、つまり、上記ＰＩＮと（ＰＩＮ）とが一致し、上記ステップＤ１におけるＰＩＮのキー入力者は、本カード１１の真の所有者であると判定されると、ステップＤ３に進み、システム制御部２２はフラグレジスタ２９に対してフラグ“１”を立てさせる。この後、ステップＤ４に進み、カード１１側ではターミナル１２側からの電源電圧Ｖｄｄの供給が有るか否かを常に検出し判断する。ここで、ステップＣ１において、ＩＣカードターミナル１２のカード挿入口１５対してＩＣカード１１の一端を挿入し、カード側の接続端子２０とターミナル側の接続端子５３との電気的接続を図ると、ステップＤ２に進み、ターミナル側の電源制御部５４からカード側に対する電圧Ｖｄｄの電源供給が開始される。すると、上記カード側のステップＤ４においてはＹ（Ｙｅｓ）、つまり電源電圧Ｖｄｄが供給されターミナル１２との完全接続状態に至ったと判断されると、ステップＤ５に進み、ＰＡＮメモリ３０より取出した口座番号ＰＡＮおよび暗号化口座番号ＰＡＮ′を、インターフェイス部３２を介してターミナル側に送信する。すると、ターミナル側では、ステップＣ３において、上記カード側より送られて来るＰＡＮおよびＰＡＮ′を受信し、ＰＡＮをＰＡＮラッチ部４７に、ＰＡＮ′を解読部４８に送込む。この解読部４８では、ステップＣ４において、ＰＵＫメモリ４９に記憶される暗号解読用のキーコードに基づき上記暗号化口座番号ＰＡＮ′を解読し、解読ＰＡＮラッチ部５０に（ＰＡＮ′）としてラッチさせるもので、この後ステップＣ５に進み、口座番号比較部５１は、上記ＰＡＮラッチ部４７にラッチされる口座番号ＰＡＮと解読ＰＡＮラッチ部５０にラッチされる解読口座番号（ＰＡＮ′）とを比較照合する。このステップＣ５においてＹ（Ｙｅｓ）、つまりカード側より送られて来るＰＡＮと本ターミナルにて解読した（ＰＡＮ′）とが一致し、現在接続中のＩＣカードは正当なものであると判定されると、ステップＣ６に進み、システム制御部４３は上記ＩＣカード１１に対してフラグ要求信号を出力する。すると、カード側では、ステップＤ６において上記ターミナル１２側からのフラグ要求信号を受信し、ステップＤ７に進んで、上記ステップＤ３にてフラグレジスタ２９に立てたフラグ“１”をターミナル側に送信する。すると、ターミナル１２側では、ステップＣ７において上記カード１１側からのフラグ信号を受信し、このフラグ信号には“１”が立っているか否かをステップ

Ｃ８にて判断する。このステップＣ８においてＹ（Ｙｅｓ）、つまり、上記ステップＣ５において、現在接続中のＩＣカード１１が正当なものであると判定されただけでなく、上記ステップＤ２において、既に上記ステップＤ１におけるＰＩＮのキー入力者は、本カード１１の真の所有者であると判定されていると判断されると、ステップＣ９に進み、システム制御部４３は表示部１４に対してカードＯＫメッセージ（ＯＫ！）を表示させる。これにより、ＩＣカード１１自体が正規に発行された本物であることおよびそのカードの持主が所有者本人であることが何れも判明することとなり、カード所有者の正当性は確実なものとなる。

一方、上記ステップＤ２においてＮ（Ｎｏ）、つまりＩＣカード１１においてキー入力したＰＩＮと予め記憶される真のＰＩＮとが一致しないと判定されると、ステップＤ８に進み、システム制御部２２はフラグレジスタ２９に対してフラグ“０”を立てさせる。この場合、上記ステップＣ５に進んだ時点においてＹ（Ｙｅｓ）、つまりカード側より送られて来るＰＡＮと本ターミナルにて解読した（ＰＡＮ′）とが一致し、現在接続中のＩＣカードは正当なものであると判定されても、ステップＣ８においてＮ（Ｎｏ）と判定され、ステップＣ１０に進む。このステップＣ１０において、システム制御部４３は表示部１４に対してカード不可メッセージ（ＢＡＤ）を表示させるもので、これにより、本ＩＣカード１１が上記ターミナル１２に正規に対応するものであっても、その所有者自体が真の所有者ではないことが確認されるようになる。この場合、本カード１１は、例えば盗難に合った可能性が高いことが判明する。

さらに、上記ステップＣ５においてＮ（Ｎｏ）、つまり接続中のカードより送られたＰＡＮと本ターミナルにて解読した（ＰＡＮ′）とが一致せず、現在接続されているカード１１は正規に発行されたものではないと判定されると、上記ステップＣ１０に進み、システム制御部４３は表示部１４に対してカード不可メッセージ（ＢＡＤ）を表示させる。これにより、上記ＩＣカード１１は、例えば偽造された擬い物の可能性が高いことが確認される。よって、本カード１１の所有者も、このステップＣ１０の時点において、正当な所有者ではないことが判明する。

したがってこのように構成されるＩＣカードにおける本人照合方式によれば、ＩＣカード１１の所有者は真の所有者であるか否かだけではなく、そのカード自体が銀行等により正規に発行されたものであるか否かをも確認することができるので、カード利用者の正当性を確実に証明することが可能である。また、上記ＩＣカード１１における暗証番号ＰＩＮの比較照合動作は、カードターミナル１２との接続時においては実行されないように構成されているので、万一、カードターミナル側に何等かの細工が施してあったとしても、カード利用者の暗証情報が盗まれる恐れは全くない。

［発明の効果］

以上のようにこの発明によれば、外部装置との接続によりカード自体の正当性が確認できるＩＣカード内に、所定文字数の暗証情報を予め記憶する暗証情報メモリを設けると共に、上記外部装置との非接続状態において上記所定文字数情報の入力可能な手段を備えさせ、そして、この入力手段により入力される所定文字数の情報と上記暗証情報メモリに予め記憶される暗証情報とをこのＩＣカード内にて独自に比較照合し、その照合結果を出力するように構成したので、カード所有者の暗証情報が不正に盗まれてしまうことなく、カード所有者の正当性を確実に認証することが可能となるＩＣカードにおける本人照合方式を提供できる。

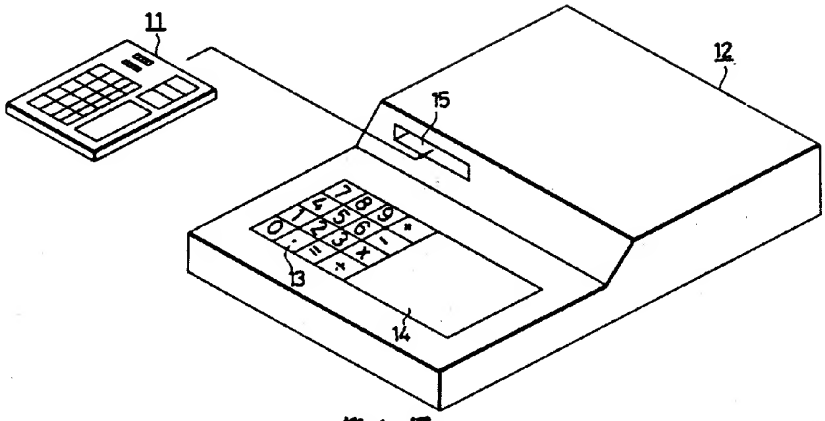
４．図面の簡単な説明

第１図はこの発明の一実施例に係わるＩＣカードにおける本人照合方式を実現した場合のＩＣカードターミナルを示す外観構成図、第２図は上記第１図におけるＩＣカードを抜出して示す外観構成図、第３図は上記ＩＣカードにおける本人照合方式を実現した場合のＩＣカードを示す回路構成図、第４図は上記ＩＣカードにおける本人照合方式を実現した場合のＩＣカードターミナルを示す回路構成図、第５図および第６図はそれぞれ上記

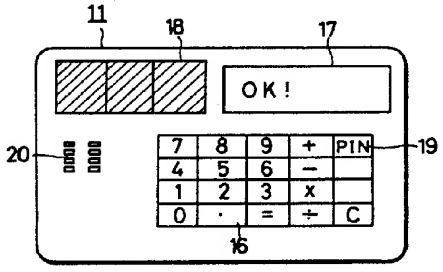
ＩＣカードにおける本人照合方式によりＩＣカードの正当性およびカード所有者が本人か否かを順次照合確認する場合の動作を示すＩＣカードターミナル（外部装置）側およびＩＣカード側のフローチャート、第７図および第８図はそれぞれ上記ＩＣカードにおける本人照合方式によりＩＣカードの正当性およびカード所有者が本人か否かを上記第５図および第６図に示した場合とは逆に順次照合確認する場合の動作を示すＩＣカードターミナル（外部装置）側およびＩＣカード側のフローチャートである。

１１…ＩＣカード、１２…ＩＣカードターミナル（外部装置）、１４…ターミナル表示部、１５…カード挿入口、１６…カードキーボード、１７…カード表示部、１８…ソーラ電池、１９…ＰＩＮキー、２０…カード接続端子、２２…カードシステム制御部、２７…ＰＩＮメモリ、２８…ＰＩＮラッチ部、２９…フラグレジスタ、３０…ＰＡＮメモリ、３１…暗証情報比較部、４３…ターミナルシステム制御部、４６…フラグ判断部、４７…ＰＡＮラッチ部、４８…解読部、４９…ＰＵＫメモリ、５０…解読ＰＡＮラッチ部、５１…口座番号比較部、５３…ターミナル接続端子、５４…電源制御部。

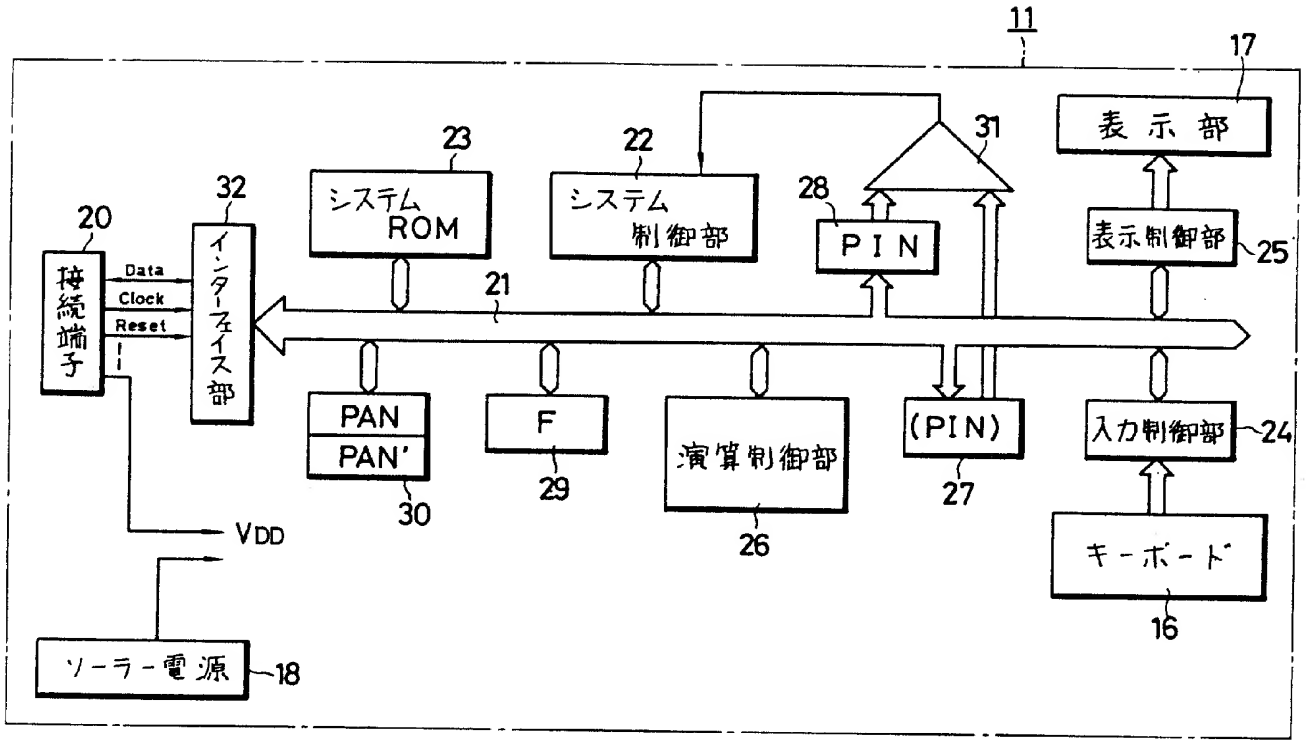
出願人　カシオ計算機株式会社



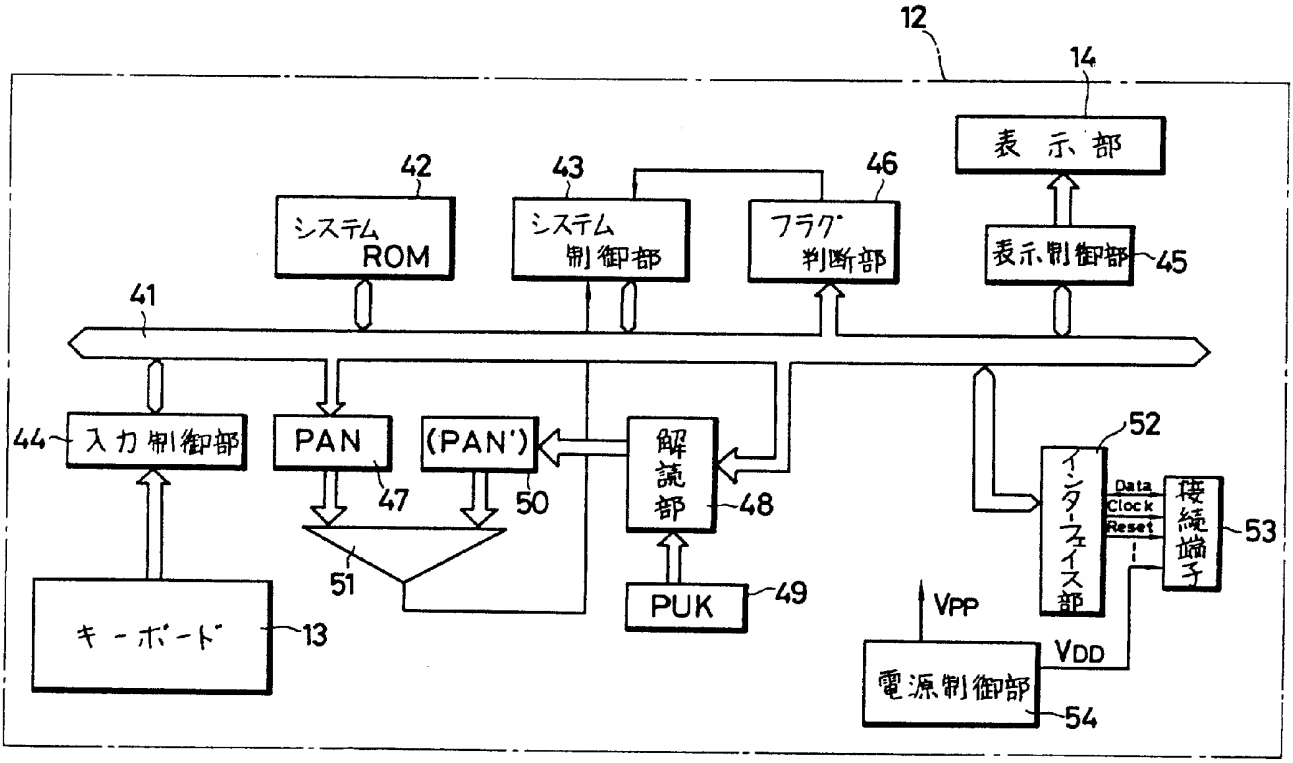
第１図



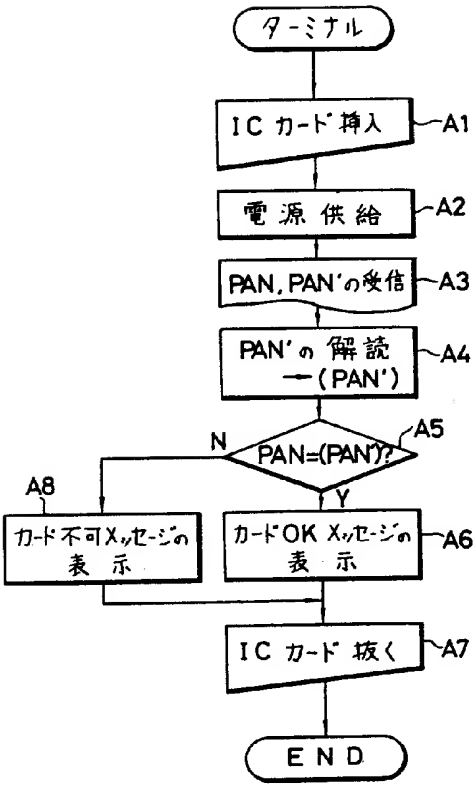
第２図


11
17
表示部
23
22
31
システム ROM
システム 制御部
28
PIN
表示制御部
25
32
20
接続端子
Data
Clock
Reset
インターフェイス部
21
PAN
PAN'
30
F
29
演算制御部
26
(PIN)
27
入力制御部
24
キーボード
16
VDD
ソーラー電源
18

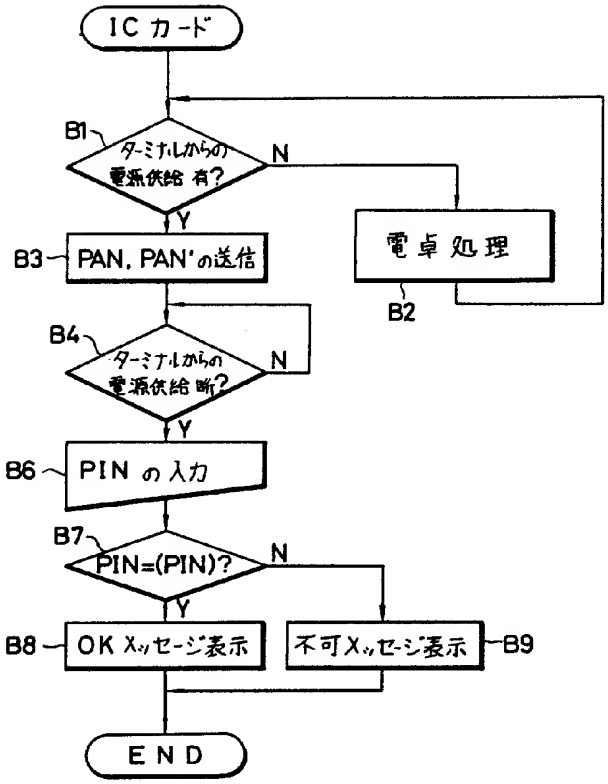
第 3 図


12
14
表示部
42
43
46
システム ROM
システム 制御部
フラグ 判断部
表示制御部
45
41
44
入力制御部
PAN
47
(PAN')
50
解読部
48
52
インターフェイス部
Data
Clock
Reset
接続端子
53
51
PUK
49
キーボード
13
VPP
VDD
電源制御部
54

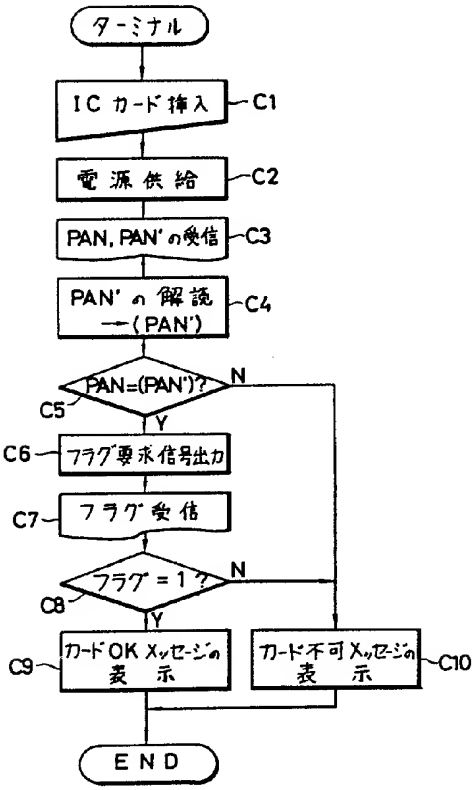
第 4 図



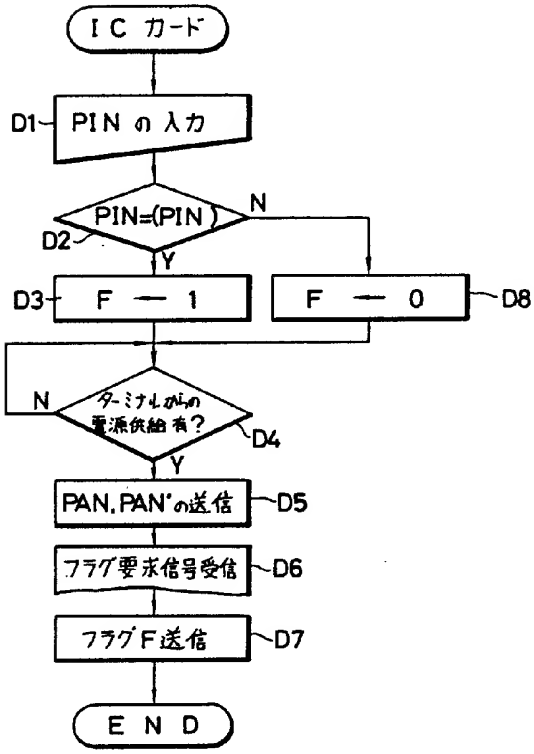
第 5 図



第 6 図



第 7 図



第 8 図